Rekontruksi Kasus Ann Skip Bail Dengan Pendekatan Prinsip Occam Razor & Alexiou
Rabu, 1 Februari 2017 | 03:40:04 WIB |

Dalam tulisan yang berhasil penulis telusuri, mengenai konsep Occam's Razor dan Alexiou yang menerangkan tentang bagaimana aplikasi pertanyaan yang benar akan menghasilkan analisis permasalahan yang lengkap sehingga solusi bisa dicapai dengan efektif dan efisien.

Banyak teori yang dapat digunakan seorang investigator untuk mengungkap suatu kasus. Saat melakukan forensika digital, ekstraksi barang bukti digital dari barang bukti elektronik (baca : digital evidence), **5W + 1H** yang disampaikan oleh William Ochkman bisa diterapkan untuk menemukan titik terang, bukti yang kuat atau petunjuk, terhadap bukti selanjutnya. Dalam teorinya menyebutkan, "The simplest answer is most often correct", dengan kata lain adalah "Jawaban yang paling sederhana adalah jawaban yang paling sering benar". Maksud dari kata "benar" di sini adalah entitas seharusnya tidak dibuat rumit jika memang tidak perlu. Occam's Razor adalah proses menyelidiki informasi sehingga dapat menemukan kebenaran dengan lebih mudah. Teori ini dikenal dengan teori Occam's Razor yang memiliki unsur-unsur **5W + 1H** yang terdiri dari "What, Who, When, Where, Why, How," yang biasa digunakan dalam sebuah artikel atau berita. Lebih luas lagi, **5W + 1H** dapat pula diaplikasikan pada hal yang lain. Kata "tanya" sebagai indikator dari sebuah analisis permasalahan dalam mengungkap sebuah peristiwa kejahatan.

Selain itu, untuk proses investigasi dapat juga menggunakan teori yang disampaikan oleh Michael Alexiou, Chief Operating Officer CyTech Services, Inc, Washington D.C., Amerika Serikat. Dimana dalam teorinya terdapat 4 prinsip yang dikemukakan, yaitu:

1. What question are you trying to answer?
2. What data do you need to answer that question?
3. How do you extract that data?
4. What does that data tell you?

Dari ke-empat prinsip tersebut, maka investigator dapat melakukan analisis sesuai dengan standard yang diperlukan. Hal ini untuk menghindari proses investigasi yang tidak terukur dan tidak meyakinkan dalam memecahkan sebuah kasus atau peristiwa.

Untuk lebih mempertajam pembahasan kedua konsep tersebut, penulis berkesempatan menjabarkan dengan sebuah kasus Ann's Skip Bail atau Ann Dercover, dimana Ann adalah seorang pegawai yang menjadi mata-mata di salah satu perusahaan dimana dia bekerja. Dan aktifitas perusahaan tersebut direkam dan di kirimkan Ann kepada temannya diperusahaan lain yang menjadi pesaing perusahaanya. Ann sendiri pada akhirnya ditangkap dengan tuduhan "menjual" informasi perusahaan kepada pesaingnya. Dalam proses penahanannya, Ann dibebaskan dengan jaminan, dan menghilang.

Setelah Ann menghilang bersama kekasihnya, investigator memeriksa aktifitas network yang digunakan Ann untuk berkomunikasi dengan kekasihnya itu sebelum menghilang. Dalam proses analisis, investigator menemukan sebuah petunjuk berupa packet capture yang bernama **"evidence02.pcap".** Paket Capture ini di digunakan pada tanggal 10 Oktober 2009, mulai dari jam 20:34:08 sampai 20:38:22 dengan rentang waktu selama 00:04:14.

File summary dari packet capture

Investigator memberikan tantangan untuk bisa memecahkan kasus ini melalui barang bukti digital yang didapat dari hasil analisa paket network pada file evidence02.pcap, berikut uraiannya :

After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.

"We believe Ann may have communicated with her secret lover, Mr. X, before she left," says the police chief. "The packet capture may contain clues to her whereabouts."

You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence including:

1. What is Ann's email address?
2. What is Ann's email password?
3. What is Ann's secret lover's email address?
4. What two items did Ann tell her secret lover to bring?
5. What is the NAME of the attachment Ann sent to her secret lover?
6. What is the MD5sum of the attachment Ann sent to her secret lover?
7. In what CITY and COUNTRY is their rendez-vous point?
8. What is the MD5sum of the image embedded in the document?

Untuk menjawab tantangan ini, kita memerlukan aplikasi pendukung seperti, Wireshark, notepad, dan Hashcalc, untuk melakukan analisis terhadap bukti digital yang diperoleh.
Setelah semua tersedia, dan berjalan dengan baik, maka lakukan langkah berikut untuk menjawab pertanyaan dari tantangan yang diberikan.

1. What is Ann's email address? sneakyg33k@aol.com

2. What is Ann's email password? 558r00lz

Lalu gunakan Base64 DECODE, dengan bantuan tools yang ada di https://www.base64decode.org/ maka akan terlihat passwordnya. Seperti gambar dibawah ini :

3. What is Ann's secret lover's email address? mistersecretx@aol.com

4. What two items did Ann tell her secret lover to bring? fake passport and a bathing suit

Untuk mendapatkan informasi ini, gunakan paket 120 lalu lihat informasi Follow TCP Stream, didalam akan terdapat informasi seperti gambar berikut :

5. What is the NAME of the attachment Ann sent to her secret lover? secretrendezvous.docx

Masih dalam paket yang sama, perhatikan nama isi file stream, berikut :

Jika kita telusuri lebih dalam lagi informasi file attachment tersebut maka akan didapat informasi penting mengenai lokasi dimana akan dilakukan pertemuan.

Dengan sedikit trik yang butuh ketelitian, dimana informasi yang tertulis dengan bahasa simbol dengan menggunakan metode EncodeBase64, maka penulis mencoba membuka isi dari file attachment tersebut dengan mencopy bagian yang di Encode. Lalu menerjemahkannya dengan bantuan plugin dari Notepad++ yaitu MIME Tools Decode64 dan menyimpannya dalam bentuk file dokumen (*.doc atau *.docx) maka informasi yang terdapat dalam file attachment yang dalam kondisi terenkripsi tersebut dapat terbaca dengan jelas. Berikut langkah-langkah yang penulis lakukan :

a. Select bagian teks dari UEsDBBQ…..sampai A9CYDAAAA

b. Copy dan Paste bagian teks yang sudah di select (pilih) dihalaman Teks Editor Notepad++

c. Tekan Ctrl+A, lalu masuk ke bagian Menu Plugins --> MIME Tools --> Base64 Decode

d. Hasil Base64Decode, isi file sudah berubah

*e. Simpan file hasil Decode tadi dengan ektensi *.doc atau *.docx, buka dengan aplikasi Ms. Word*

Hasil DECODEBASE64 dengan bantuan plugins dari Notepad++

Hasil Save-AS berupa file dokumen yang berisi informasi lokasi pertemuan.

6. What is the MD5sum of the attachment Ann sent to her secret lover?
9e423e11db88f01bbff81172839e1923

7. In what CITY and COUNTRY is their rendez-vous point? Playa Del Carmen, Mexico

8. What is the MD5sum of the image embedded in the document?
57c44bb5d383d43751b83787d1934569

Dengan terjawabnya pertanyaan yang diberikan oleh investigator tersebut, maka penulis merangkumnya dalam bentuk kesimpulan dari kedua teori diatas, yaitu :

A. OCCAM'S RAZOR PRINCIPLE

WHAT :

Apa yang terjadi dengan kasus yang sedang ditangani. Kasus yang sedang ditangani adalah seorang karyawan yang telah melakukan tindakan mata-mata dengan memberikan informasi mengenai aktifitas perusahaan dimana karyawan itu bekerja kepada temannya yang bekerja di perusahaan saingannya. Hal ini dianggap sebagai tindakan kejahatan cybercrime.

WHEN :

Informasi yang didapat dari packet capture pada 10 Oktober 2009, mulai dari jam 20:34:08 sampai 20:38:22 dengan rentang waktu selama 00:04:14

WHERE :

Dari informasi packet capture Ann bersama kekasihnya bertemu di kota Playa del Carmen, Mexico.

WHO :

Pihak yang terlibat dalam kasus ini, berdasarkan informasi packet capture yang ada, maka ditemukan 3 (tiga) alamat email yang terdiri dari:

1) Alamat email pelaku : sneakyg33k@aol.com
2) Alamat email teman pelaku : sec558@gmail.com
3) Alamat email kekasih pelaku : mistersecretx@aol.com

WHY :

Mengapa kasus ini terjadi. Kasus ini terjadi berawal dari aktifitas Ann yang mengirimkan informasi rahasia kepada temannya di perusahaan lain melalui email. Akibat dari perbuatannya ini, Ann dijerat hukuman penjara, tapi dibebaskan dengan jaminan dan dikenakan wajib lapor.

HOW :

Bagaimana Ann bisa ditemukan. Karena statusnya yang mengharuskan wajib lapor, maka pelaku berusaha "menghilang" dan itu sangat menyulitkan aparat hukum dalam menginvestigasi kasus ini lebih dalam lagi. Akhirnya, investigator menemukan packet capture yang berisi attachment dimana didalamnya menginformasikan sebuah alamat untuk melakukan pertemuan. Informasi ini didapat dari network yang digunakan pelaku selama melakukan kegiatan "spionase". Dan informasi didapatkan bahwa pelaku bertemu dengan kekasihnya di Mexico.

B. ALEXIOU PRINCIPLE

1) WHAT QUESTION ARE YOU TRYING TO ANSWER?

Pertanyaan apa saja yang harus investigator jawab dalam usaha memecahkan suatu kasus. Dari kasus ini investigator telah merangkum 8 (delapan) pertanyaan yang berisi :

a. What is Ann's email address?
b. What is Ann's email password?
c. What is Ann's secret lover's email address?
d. What two items did Ann tell her secret lover to bring?
e. What is the NAME of the attachment Ann sent to her secret lover?
f. What is the MD5sum of the attachment Ann sent to her secret lover?

g. In what CITY and COUNTRY is their rendez-vous point?
h. What is the MD5sum of the image embedded in the document?

2) WHAT DATA DO YOU NEED TO ANSWER THAT QUESTION?

Data apa yang investigator butuhkan dalam memecahkan kasus tersebut. Dari kasus yang ada, data yang ditemukan dalam packet capture adalah file evidence02.pcap. Dari bukti digital inilah kemudian dianalisis informasi yang terdapat didalamnya.

3) HOW DO YOU EXTRACT THAT DATA?

Bagaimana investigator dapat mengurai data dari file yang ditemukan tersebut untuk dijadikan sebuah informasi yang berguna dalam mengungkap kasus ini. Dengan bantuan beberapa tools, diantaranya WireShark, Notepad++, HashCal, dan lainnya. Maka data tersebut berhasil di urai dan menghasilkan informasi yang sangat berguna untuk mengungkap kasus ini.

4) WHAT DOES THAT DATA TELL YOU?

Informasi apa yang didapat setelah data berhasil diurai. Dari hasil investigasi berdasarkan barang bukti digital yang ada, maka investigator dapat menjawab 8 (delapan) pertanyaan yang sudah dirangkum sebelumnya.

Dari penjelasan diatas, penulis semakin yakin dengan apa yang diungkapkan oleh Dr. Edmon Locard dalam teorinya yang mengatakan bahwa, “Every contact leaves a trace”. (baca : Hubungan Prinsip Locard Exchange Dengan Digital Forensic). Setiap bentuk kejahatan, akan meninggalkan jejak, bukti fisik tidak bisa salah, tidak bisa bersumpah palsu, dan tidak sepenuhnya tidak ada. Hanya kegagalan manusia untuk menemukannya, mempelajari dan memahaminya, yang dapat mengurangi nilainya.

Dalam peristiwa kejahatan, benda ataupun jejak yang memiliki keterkaitan dalam suatu peristiwa dapat dijadikan barang bukti ataupun petunjuk dalam mengungkap kasus dari suatu peristiwa kejahatan. Sebagaimana penulis telah sampaikan dalam tulisan sebelumnya mengenai barang bukti (baca : Antara Cybercrime dan Cyber Computer). Hal inilah yang dapat membantu dalam pengungkapan suatu kasus kejahatan dari bukti forensik yang ada.

Sumber :

- Lih., Joseph M. de Torre, Christian Philosophy, Manila, Sinag-Tala Publishers, 1980, Hlm. 30
- Occams Razor – The Skeptics Dictionary
- Shuttleworth, M. (2008, July 26). Occams razor – the simplest answer is usually correct
- The digital standard: The alexiou principle [Web log post]. (2009, June 27)
- Problem Solving Investigations
